This is an author version of a conference paper which was first published in July 2008 in K. Michael and M.G. Michael eds., Australia and the New Technologies: Evidence Based Policy in Public Administration, University of Wollongong Press, Wollongong, pp. 24-31. See http://www.homelandsecurity.org.au/publications.html for published version.

Profiting from personal information: Power, information privacy and evidence based policy

Mark Burdon
PhD Candidate/Research Associate, Faculty of Law/Information Security Institute, Queensland University of Technology

Abstract

The difficulties that emerge when governments attempt to commercialise personal information are shown by the sale of home owner details in Queensland. Solove contends that such difficulties arise because of power differences between government organisations, private sector companies and individuals. The development of effective policy responses, particularly those regarding the sale of personal information, must identify and address power issues inherent in information privacy problems.

Keywords: Information privacy, power, decision making, accountability, transparency.

1 Introduction

The public sector has a large number of databases containing personal data such as names, addresses and ages. In the UK, it has been estimated that there are 300 million personal data records - on average five sets of personal data for every citizen (Council for Science and Technology 2005, 6). This highlights the unique position that governments have as the primary collector of public data (OECD 2006). Government organisations have statutory means to enforce disclosure and they are the only feasible provider of comprehensive national data sets (Rowlands 1995, 227). Concurrently, the enhanced development of information and communication technologies in government has created new opportunities for agencies to collect, share and re-use data. As a consequence, the commercial worth of governmental data sets and value added information products/services have increased (PIRA International 2000). Government organisations are now finding that data which they have routinely collected to fulfil their statutory and business functions can now more easily be re-used for commercial purposes (Office of Fair Trading 2006). As such, the commercialisation of public sector information, including personal information, has been a part of the developing information economy which is believed to generate annual worldwide revenues in the hundreds of billions of dollars (Somogy 2006, 904).

However, the commercialisation of personal information by governments can create information privacy problems as highlighted in the next section. Solove argues that such problems occur from the imbalance of power relationships between individuals and organisations. Section 3 examines Solove's claims and Section 4 applies his analysis to the Queensland problem. Section 5 looks further into the relationship between power and privacy and suggests that a different form of policy research could be used for evidence based policy development. Finally, the author briefly concludes the paper about how such an approach could help to factor in underlying power mechanisms involved in information privacy problems and thus lead to the further development of information privacy laws.

2 A Queensland information privacy problem arising from the sale of personal information

The recent Federal Court case of *RP Data v State of Queensland [2007] FCA 1639* highlights some major concerns for government organisations regarding the re-use of personal information for income generation purposes. The Department of Natural Resources and Mines (now Department of Natural Resources and Water and hence referred to as NRW) is mandated by law to collect and maintain information on real property valuations arising from obligations under the Valuation of Land Act (QLD) 1994 (hence referred to as the VLA) and land title information under the Land Titles Act (QLD) 1994. Section 37 of the VLA requires NRW to conduct an annual valuation of the unimproved value of all land in local government areas and to record details of valuation in a roll. The valuation roll contains information such as a property owners name and

address; the situation, description and measurement or area of the land; a valuation of the unimproved value and additional details required under section 47 of the VLA.

Further statutory requirements arising from the VLA also oblige NRW to supply valuations data in various forms. For example, section 73 requires the Chief Executive of NRW to provide a copy of the valuation roll to various administrative parties such as the Commissioner of Land Tax. Section 77 of the VLA establishes the context in which NRW can sell valuation information. The Chief Executive is entitled to embark on contractual relations with third parties for the supply of valuation roll information in the form of bulk data products. For the purpose of the legislation, bulk data is defined as at 20% of all land parcels in Queensland or all section 81 information for parcels of land in Queensland.

NRW combined the valuations data with data collected on property sales to create the Queensland Valuation and Sales (QVAS) dataset which was first supplied under licence to RP Data, an information broker, in 1992. RP Data was one of eight information brokers used by NRW to distribute QVAS but it was by far the biggest with a 70% share of the information market. RP Data was effectively a non-exclusive data broker for NRW and value added the QVAS data into a more commercially friendly product that was sold, predominantly to real estate agents, but also to other government departments. Interestingly, at the onset of the relationship, RP Data informed NRW of the possibility that value added information may be used for direct marketing by real estate agents and the agency was prepared to contemplate that use. However, this was not the case 10 years later, when NRW sought a change of policy.

During the intervening years, NRW received a number of complaints regarding the use of personal information provided to the agency that had been re-used by real estate agents for direct marketing purposes. This led to the instigation of section 27 of the Land Legislation Amendment Act (QLD) 2003 which sought to prohibit the use of direct marketing, using names and addresses supplied by NRW in the QVAS dataset. Section 27 inserted two subsections into the VLA. Section 77(3)(A)(a) allowed the Chief Executive of NRW to exclude elements of the valuation roll information provided under contract if he/she “"is satisfied, on reasonable grounds, that inclusion of the particulars may result in the particulars being inappropriately disclosed or used”. Section 77(3)(A)(b) provided a retrospective power to prohibit disclosure or limit distribution and use of supplied information.

The advent of section 77(3)(A) led to a new licensing agreement between NRW and the 8 information brokers which came into effect in July 2003. The new licence had four new clauses that directly prohibited direct marketing of NRW’s QVAS dataset. Clause 4.4.2 required the licensee to acknowledge and to be bound by restrictions that did not allow licensed data, consisting of details identifying individuals (e.g. names and addresses), to be used for direct marketing. Clause 4.5.2 required the licensee not to distribute the licensed data to a third party for direct marketing purposes. Furthermore, clauses 4.10.2 and 4.11 required that the licensee must not distribute the licensed data to an end user unless that party has entered into an agreement not to use the data for direct marketing. Finally, clause 9.11 affirmed the right of the licensor to exclude elements of QVAS data on reasonable grounds of inappropriate use or disclosure (e.g. direct marketing).

Despite the new licensing agreement, the QVAS data continued to be used by real estate agents for direct marketing purposes and NRW received 219 written complaints and numerous phone calls from members of the public. Additional complaints were also received by real estate agents who were 'doing the right thing' by adhering to NRW's licence requirements and managing agents of unit complexes. The lack of compliance with the new licence prompted NRW in July 2005 to exclude the provision of names and addresses in the QVAS dataset. The purpose of which was explained by NRW's Director of Product Services in his affidavit to the court:

> "15. The purpose of making a new proposal to withdraw names and addresses from the bulk data was as a consequence of complaints received from various individuals that their personal details had been obtained by direct marketers and they were concerned about Government information being used in inappropriate ways."

RP Data then brought an action against NRW under section 46 of the Trade Practices Act (Cth) 1974 on the grounds that NRW had abused its market power by withdrawing names and addresses from QVAS. The grounds of the action are beyond the scope of this paper but it is worth noting that judgment was found for NRW on the basis that the removal of names and addresses was not based on anti-competitive behaviour but on a desire to ensure that NRW's information was not used improperly.

It is somewhat surprising that concerns about the commercialisation of personal information have not come to the fore at an earlier stage. Larson (1994, 40-44) highlights that the re-use and sale of census data in the US started in the late 1960's and was a major contributing factor to the development of direct marketing tactics. Large-scale, publicly collected datasets were merged and re-formatted into new mailing lists, used specifically for targeting customers and sending mail shots. Moreover, recent research conducted for the UK Government has suggested that formal information privacy principles are required to ensure the governance of enhanced information sharing. As a consequence, government organisations should not be allowed to sell public sector personal information to commercial organisations (OPM 2005, 14). However, identifying the actual causes of such problems and anxieties are perhaps not as clear cut as can first appear due to the inherent issues of power underlying the relationship between individuals and bureaucracies that are manifest in information privacy concerns.

3 Metaphors of power

Solove (2001) contends that information privacy problems, similar to those encountered in Queensland, are best explained as arising from unbalanced power relationships between individuals and organisations. More specifically, issues of mass personal data collection are grounded in an outdated paradigm of information privacy as a Big Brother problem. This metaphorical view, based on Orwell's '1984', depicts privacy problems as invasions of privacy through surveillance. Or in the context of databases, through 'dataveillance' (Clarke 2006) which is the systematic collection and use of personal and non-personal data by bureaucracies for surveillance purposes (Solove 2001, 1417). Whilst this view has been dominant amongst most privacy legal theorists and law makers, Solove contends that a more appropriate metaphor, to view privacy

problems arising from the use of databases, emerges from a view of privacy based on Kafka's 'The Trial'.

The Big Brother metaphor provides a narrow view of the application of information privacy in society. In 1984, the fictional state of Oceania is dominated by an omnipotent and all knowing governmental bureaucracy encapsulated by its dictator leader, Big Brother. Each citizen's life is strictly regulated as Big Brother controls all aspects of existence. Collective uniformity is gained through absolute obedience founded on fear of punishment and execution. The concept of personal privacy is eradicated as Big Brother exercises power through constant surveillance via the obsequious 'telescreen' thus leading to the elimination of private thoughts. Privacy using the Big Brother metaphor therefore represents the use of coercive power by governments to oppress, control and dominate (Solove 2001, 1415).

Solove argues that the Kafka metaphor offers a more realistic analysis of the information privacy concerns relating to databases and the power issues entailed. In The Trial, an individual, Joseph K is notified that he has been arrested for an unnamed offence. Outraged and perplexed, he embarks on a quest to ascertain why he has been arrested and who is behind his arrest. Joseph K encounters a bureaucratic legal system that is indifferent to the needs of individuals, is devoid of purpose and exercises power for no apparent goal or reason (Solove 2001, 1423). In real life, Solove contends that the primary information privacy problem with databases stem from the way the bureaucratic process treats individuals and their information (Solove 2001, 1421). Especially bureaucracies and bureaucratic processes that have little intelligent control or limitation which result in a lack of meaningful participation by individuals regarding the decisions to collect and use their personal data (Solove 2001, 1422).

There are significant differences between conceptualisations derived from both the Big Brother and Kafka metaphors. However, the use of both metaphors conceives information privacy issues as problems of power. The Big Brother metaphor is concerned with the direct exercise of power by bureaucratic organisations to coerce individuals. Power in the Big Brother sense involves dictatorship, control and enforced obedience. Whereas the Kafka metaphor focuses on the imbalance of power relationships between helpless individuals and uncaring bureaucracies that make decisions and enact without any meaningful purpose or design. Under the latter, Solove is referring to the information privacy dangers arising from neglectful, ill-conceived and disempowering administrative practices that govern the collection, storage and use of personal data. Solove's metaphorical analysis of information privacy as power is particularly pertinent to the issue of the re-use of personal information, held by government agencies, for income generation purposes. In terms of the commercialisation of personal information, such actions highlight the complex and shifting balance of power relationships between government departments, data brokers, commercial entities and individuals. The next section will apply Solove's metaphors to the Queensland example highlighted above to outline the operation of power relationships emanating from information privacy problems arising from the sale of personal information.

4 A power analysis of the Queensland example

Using Solove's metaphors, it would appear that the problem highlighted above is much more akin to a Kafka rather than a Big Brother type concern. The sale of the QVAS dataset by NRW and the subsequent purchase and re-use by RP Data was not conducted for reasons of surveillance and was not intended to impose control of those persons who provided their personal information. The overt focus on surveillance intrinsic in the Big Brother metaphor ignores the practical reasons that the majority of personal data is collected for. Bureaucratic personal data collection is not purely aimed at gaining control over a populace. Instead, the goal of much personal data collection, particularly its use by the private sector, is aimed at studying and exploiting our expressions of individuality rather than attempting to suppress them (Solove 2001, 1419). This point can be seen clearly in the re-use of the QVAS dataset by RP Data and estate agents, which was used for commercial purposes (e.g. direct marketing) rather than oppressive attempts of control.

Solove also contends that bureaucratic personal data collection and use is conducted by a myriad of 'Little Brothers' (Lyon 1994) for a wide-range of purposes rather than by one omnipotent government agency for one purpose (Solove 2001, 1421). Solove argues that the world is essentially controlled by bureaucracies and the important factor to be considered regarding the collection of personal data is the relationship between individuals, society and the 'Little Brothers'. Bureaucratic databases, and the data held in them, are integral to government and commercial decision-making, and to that extent, exacerbate and transform the power relationships between individuals and bureaucracies (Solove 2001, 1422). This diffusion of data collection and use highlights the fact that the majority of personal data collected does not actually have an embarrassing element and that most people are happy to part with seemingly innocuous personal details. The Queensland example re-emphasises this point. The primary act of data collection was done so by NRW under the auspices of the VLA that compelled individuals to provide personal data and mandated the agency to collect it. It was not until the subsequent re-use of the primary personal data, first by NRW to produce the QVAS dataset and then by RP Data and real estate agents, for commercial purposes that the provision of "seemingly innocuous personal details" was suddenly perceived in a new light.

This highlights that information privacy problems occur from a group of disempowering practices associated with the collection and use of personal data (Solove 2001, 1425). Solove argues that a precondition for successful information privacy regulation must be to establish rules that govern the power relationships between individuals and bureaucracies (Solove 2001, 1455). Such rules should seek to equalise power imbalances and thus ensure the instigation of fair, voluntary and informed information transactions. In the Queensland example, it would appear that these rules were not given enough weight by the organisations involved. Complaints from individuals did not emanate until certain acts of re-use, i.e. direct marketing, started to attract the annoyance of those persons who provided their personal information for a specific purpose only for it to be used later for a totally different purpose.

For Solove, the information privacy problems arising from mass personal data collection and the use of bureaucratic databases regard the power relationships between individuals, societies and bureaucratic organisations. Particularly as the relationship an individual has to a bureaucracy, even a benign one, about the data collected from and

about them, can have a potentially debilitating effect (Solove 2001, 1423). An interesting point that arises from the Queensland example is the fact that, at various stages of the problem, NRW was powerless to stop the re-use of personal information held in their possession for direct marketing. At those times, the government organisation was debilitated as well as the individuals in question. This highlights the complex web of power relations between 'Little Brothers' and individuals in which all parties exerted some form of power over the others. For example, individual complaints made NRW take action to withdraw personal information from RP Data, who in turn, was not able to use the QVAS dataset for the development of information products for real estate agents. Accordingly, all parties appear to have been able to exert power over the others at varying stages in the episode.

In some ways, this goes beyond traditional notions of information privacy that focus on one-to-one relationships of control over information that have been shaped within a property rights paradigm revolving around notions of ownership of personal data (Solove 2001, 1446). Solove argues that the use of this paradigm has skewed perspectives of information privacy because it focuses on balancing competing economic values between the bureaucratic organisation, that collects and holds the information; the value an individual puts on the information and the larger social value of individual's maintaining control of their information (Solove 2001, 1446). This point can be seen clearly in the Queensland example. The problem appears to have emerged due to a combination of certain factors: (a) NRW's original decision to commercialise information, including personal information (b) individuals were not informed that their personal information was being sold (c) the subsequent re-use of personal information, by another body, for direct marketing purposes. It would appear that at various stages, the economic considerations of those organisations involved outweighed the societal value of maintaining control of personal information. It is not until the point where individuals start to value the use of their personal information that the latter, at least in terms of NRW's involvement, started to outweigh the former.

5 Power, information privacy and evidence based policy

Once the notion of power as an element of information privacy is applied, the underlying foundations of information privacy law no longer appear suitable to resolve current and future problems because of the dominant paradigms of surveillance and ownership which continually divert attention away from the real problem - the imbalance of power relationships (Solove 2001, 1431). However, like privacy, the concept of power has been notoriously difficult to define (Lukes 2005, 61) (Dyrberg 1997, 1) which is why it has perhaps received so little academic discussion in the US and in Australia.

Ehrenreich (2001) argues that power has not been discussed in tandem with privacy because of the imprecise nature of power, particularly in the form of Marxist discourse, that has largely been discredited in the US (Ehrenreich 2001, 2057). As a result, to speak of power in modern America is akin to saying something distasteful because it reminds Americans of inequalities that they would rather not acknowledge. Power is hard to talk about, but privacy is not because "the notion of privacy resonates well in a country so heavily seduced by the notion of 'individual freedom'" (Ehrenreich 2001, 2057). It is

difficult for the American political discourse to distinguish fully between privacy and power because both concepts are so intimately bound together (Ehrenreich 2001, 2058)

> "[I]t would probably not be an exaggeration to say that without privacy, power could not sustain itself; and without power, privacy could not exist. As I argue in the remainder of this Review Essay, the realm of the "private" is always constructed in relation to social power: Power constructs privacy and, to maintain itself, power also destroys privacy. Privacy, in turn, both constructs power and challenges it."

As regards the Australian literature, Lindsay (2005) has addressed Foucauldian concepts in the wider context of Australian information privacy laws and contests that the issue of power and privacy has yet to be fully explored (Lindsay 2005, 140). He argues that Foucault's analysis of power may assist in explaining some of the difficulties encountered with defining the concept of privacy (Lindsay 2005, 139). In so doing he defines Foucault's conception of power as

> "In his [Foucault's] view, conceiving power solely in terms of a struggle between state repression and individual liberties ignores more insidious techniques through which power is exercised in everyday life." (Lindsay 2005, 138)

Power is not purely about negative applications in the form of repression. Foucault's contention is that power can also have a positive effect because it can be used to produce knowledge and facilitate discourse. Lindsay states that Foucauldian notions of power are relevant to information privacy concerns because they highlight that the concept of privacy is really "concerned with techniques of power that are dispersed within society, and which takes a diversity of forms" (Lindsay 2005, 139). As such, "if power relationships are everywhere, then privacy, which must be seen in the context of such relations, is an understandably diffuse concept, capable of multiple meanings." (Lindsay 2005, 139).

This raises a number of challenges for evidence based policy about information privacy problems arising from the sale of personal information and such problems generally because of the invisible and conflicting nature of one of the potential causes – underlying power relationships. Policy responses therefore have to pay regard to the limits of traditional ontological and epistemological assumptions about the nature of social reality which dictate the methods of knowledge acquisition. Put simply, if underlying power relations are not conceived as a cause of information privacy problems then they will never be identified as such. Legislative and policy responses will continue to be developed but they may not be effective because one of the main underlying issues, is at best, addressed in a tangential manner. What is required, therefore, is a way of thinking about policy problems that is able to identify and address invisible causal mechanisms, such as power, that are fundamental to resolving the concern at heart.

Pawson and Tilley (1997) have applied a critical realist approach to examine policy responses implemented to reduce car park crime through the use of closed circuit TV (CCTV) cameras. Critical realist research builds models of mechanisms to be adopted as hypothetical descriptions used to reveal underlying causal mechanisms (Blaikie 2006). The research task is to demonstrate the existence of the explanatory mechanisms postulated and explanation is constructed in terms of how causal mechanisms produce events (Blaikie 2000). The guiding metaphors are therefore structures and mechanisms of reality rather than the rigorous observation of a phenomenon or event (Robson 2002, 32).

The authors argued that the use of CCTV cameras in car parks worked, not because of their presence alone, but because they triggered a chain of reasoning and response in the minds of would be thieves that inhibit illegal actions (Pawson and Tilley 1997, 78). The purpose of realist evaluation is therefore to develop a comprehensive theory of how the implementation of CCTV impacts on the thought process of the criminal mind and what combination of causal mechanisms and actual contexts produce the most effective inhibitor to car park crime. For example, CCTV could reduce car park crime because it (a) makes it more likely that an offender will be observed (b) may produce evidence that can be used in a future court action; (c) allows security resources to be allocated immediately and more effectively; or (d) may appeal to drivers to be extra vigilant regarding the security of their vehicle.

It is also possible for other causal mechanisms to exist and it is also possible that these and other mechanisms can exist at the same time. Which particular mechanism or combination of mechanisms most influences the criminal mind in turn may depend on the context for which the CCTV is installed (Pawson and Tilley 1997, 79). For example, if the car park is isolated and has little or no security, the ability to apply resources immediately is diminished and the car park operators are more reliant upon the deterrent of being able capture criminal activity on camera. This clearly provides a more limited response in contrast to a busy, security resourced car park because the latter offers a greater number of mechanisms that can inhibit the potential car thief by influencing their thought patterns. The authors contend that such an approach reveals that a bit of lateral thinking in the realm of hypothesis making frames the search for data and the application of research strategies and thus call upon the use of a range of evidence entirely different from traditional methods (Pawson and Tilley 1997, 80).

A similar approach to Pawson and Tilley's could be applied to information privacy policy evaluation to assist the identification of power mechanisms as a cause of information privacy problems, particularly those arising from the sale of personal information. Policy makers and policy analysts would be required to search for different forms of evidence that go beyond the implementation of information privacy laws and simple measurement of outcomes, generally in the form of legal actions or complaints. Instead, a much deeper evidential search would be required to examine the effects of unbalanced power relationships on the interplay between the providers, collectors and users of personal information.

The acquisition of new evidence could unveil the complex interplay of hidden mechanisms involving individuals and organisations, such as the demands for governments to be economically self-sufficient, the increasing value that the information market puts on personal information and the angst that is generated when personal information is used beyond the bounds that it is collected for, particularly direct marketing. Ultimately, this could show the limits of current information privacy laws that are founded on notions of ownership and which do not sufficiently acknowledge the existence of the power relations that are intrinsic to information privacy issues.

6 Conclusion

This paper has sought to highlight the relationship between power and information privacy within the context of an information privacy problem arising from the sale of

personal information. Such issues and the relationships entailed are clearly complex given the amorphous nature of both concepts. The effective resolution of information privacy problems, such as the one highlighted above, requires policy responses that consider new ways of thinking to address underlying causes particularly those that emerge from power imbalances.

A new way of thinking about the causes of information privacy problems could ultimately result in laws that develop informed disclosure by organisations which are founded on meaningful participation by individuals and go beyond notions of individual or corporate information ownership. It is therefore important that the development of information privacy laws focus on the structure of power in modern society and how to govern power relationships between individuals and bureaucracies regarding the collection and use of personal data. As Solove (2001, 1461) comments,

> "The problem with databases is not our being watched, controlled, or inhibited. Nor is it our lack of ownership in our personal information. Rather, it is a problem that involves power and the effects of our relationship with public and private bureaucracy - our inability to participate meaningfully in the collection and use of our personal information. As a result, we must focus on the structure of power in modem society and how to govern such relationships with bureaucracies."

References

Blaikie, N. 2000. *Designing Social Research: the Logic of Anticipation*. Cambridge, UK; Malden, MA: Polity Press.

Blaikie, N. 2006. *Approaches to Social Enquiry: Advancing Knowledge*. Cambridge, UK: Polity Press.

Clarke, R. 2006. *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*. http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html (accessed 30 April, 2007).

Council for Science and Technology. 2005. Better Use of Personal Information: Opportunities and Risks. London, UK: Council for Science and Technology.

Dyrberg, T. B. 1997. *The Circular Structure of Power: Politics, Identity, Community*. London; New York: Verso.

Ehrenreich, R. 2001. Privacy and Power. *Georgetown Law Journal*, 89 (6): 2047-2062.

Larson, E. 1994. *The Naked Consumer: How Our Private Lives Become Public Commodities*. New York: Penguin.

Lindsay, D. 2005. An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law. *Melbourne University Law Review* 29 (1): 131-178.

Lukes, S. 2005. *Power: A Radical View*. 2nd ed. Houndmills, Basingstoke, Hampshire: New York: Palgrave Macmillan.

Lyon, D. 1994. *Electronic Eye: The Rise of Surveillance Society*. Minneapolis: University of Minnesota Press.

OECD. 2006. OECD Workshop on Public Sector Information: Summary: DSTI/ICCP/IE(2006)14.

Office of Fair Trading. 2006. The Commercial Use of Public Information (CUPI). London: Office of Fair Trading.

OPM. 2005. Research into the Use of Personal Datasets Held by Public Sector Bodies. London, UK: Council for Science and Technology.

Pawson, R. and N. Tilley. 1997. *Realistic Evaluation*. London; Thousand Oaks, Calif.: Sage.

PIRA International. 2000. Commercial Exploitation of Europe's Public Sector Information - Final Report. Leatherhead, Surrey, UK: European Commission, Directorate General for the Information Society.

Robson, C. 2002. *Real World Research: A Resource for Social Scientists and Practitioner-researchers*. 2nd ed. Oxford; Malden, Mass.: Blackwell Publishers.

Rowlands, I. 1995. Toward Public-Private Synergy in the European Information Services Market. *Journal of Government Information*, 22 (3): 227-235.

Solove, D. J. 2001. Privacy and Power: Computer Databases and Metaphors for Information Privacy. *Stanford Law Review*, 53 (6): 1393-1462.

Somogy, D. J. 2006. Information Brokers and Privacy. *I/S: A Journal of Law and Policy for the Information Society*, 1 (2/3): 901-925.